



November 16, 2017

Office of Consumer Affairs and Business Regulation
501 Boylston Street, Suite 5100
Boston, MA 02116



Re: Notice of Data Security Incident

Dear Sir or Madam,

We write to inform you that the computers of Schachter Harris LLP were subject to an attack by unknown criminals that could potentially involve Massachusetts residents who filed or were involved in certain lawsuits alleging asbestos-related injuries. While we remain uncertain of the extent of the breach, as a precautionary matter, we are notifying you of this incident. We have reported the crime to and have been cooperating with the FBI in its ongoing investigation.

Schachter Harris, LLP is a Texas law firm that has served as science expert counsel for a defendant in personal injury cases alleging asbestos-related injuries. The firm does not maintain an office in your state, and all cases for which we were involved for this client were defended by local counsel in the jurisdiction where they were filed. In connection with our limited role, we received documents related to the expert issues in the cases that had been brought against our client, including pleadings, interrogatory answers, depositions, briefs, exhibits, and other materials. These documents can, depending on the case, contain information about the plaintiff or other persons involved in the case such as name, address, driver's license number, social security number, military and employment records, medical records, and medical information. Copies of documents we received about these cases were stored on our computers. Some of the cases from which we have documents were cases filed in Massachusetts or were cases involving Massachusetts residents. We have notified the client we represented in these cases.

The attackers used encryption ransomware to make some information on our computers inaccessible to us, including information we maintained in the capacity identified above. When we did not pay the ransom, the criminals claimed to possess the data from our computers. Based on our investigation, we believe that the attackers were able to acquire some files stored by our firm, relating to at least one of our clients. Based on information currently available to us, we believe that the security incident took place between August 29, 2017 and September 25, 2017. We are conducting a review of the potentially affected records and computer systems, and we have taken steps to protect data from further unauthorized access, including replacing affected systems and machines. We also are working closely with IT experts to investigate and properly address the incident.


Because of the encryption by the ransomware attack, we cannot compile a definitive list of persons whose information may have been in the files that are now encrypted. Furthermore, we do not maintain a database that contains the addresses of the plaintiffs in the cases from which we have documents. Yet, we have endeavored to identify persons whose lawsuits were filed in Massachusetts and have sent notice to a law firm that represented each person so identified. At this time, the number of residents in the commonwealth affected by the incident is unknown.

Finally, we respectfully note that by sending this precautionary notice, the firm is not stating that notice from the firm to you or to any residents of your state is required or that the firm is subject to the jurisdiction of the courts of the state to which this notice applies.

If you have any questions, please contact us at the number listed above.

Respectfully,

Schachter Harris, LLP

By: 
Cary Schachter
Ray Harris

By Certified Mail

Hotchkiss, Anne (SCA)

From: Ray Harris <rharris@shtriallaw.com>
Sent: Tuesday, January 09, 2018 11:46 AM
To: Hotchkiss, Anne (SCA)
Subject: Re: Data breach - 12170

Good morning, Ms. Hotchkiss.

Nine were sent on 11/22, and four were sent on 11/29.

-Ray

Ray Harris
Schachter Harris, LLP
909 Lake Carolyn Parkway
Suite 1775
Irving, Texas 75039
214.999.5700
rharris@shtriallaw.com

From: "Hotchkiss, Anne (SCA)" <anne.hotchkiss@state.ma.us>
Date: Tuesday, January 9, 2018 at 9:14 AM
To: Ray Harris <rharris@shtriallaw.com>
Subject: RE: Data breach - 12170

Hello Ray,

Thank you for this information. Would you please let me know the date the precautionary notices were sent out?

Thank you,

Anne

From: Ray Harris [mailto:rharris@shtriallaw.com]
Sent: Monday, January 08, 2018 4:13 PM
To: Hotchkiss, Anne (SCA) <Anne.Hotchkiss@MassMail.State.MA.US>
Subject: Re: Data breach - 12170

Ms. Hotchkiss,

Thank you for your e-mail below following up on our firm's November 16, 2017 letter to your office.

The number of Massachusetts residents potentially affected by the incident remains unknown for reasons described in our letter. Based on information received through the additional efforts also described in our letter, however, we have sent precautionary notices to 13 persons we believe to be residents of your state. Each was in the form of the attached template.

Please let us know if you have additional questions.

-Ray

Ray Harris
Schachter Harris, LLP
909 Lake Carolyn Parkway
Suite 1775
Irving, Texas 75039
214.999.5700
rharris@shtriallaw.com

From: "Hotchkiss, Anne (SCA)" <anne.hotchkiss@state.ma.us>

Date: Monday, January 8, 2018 at 10:35 AM

To: Ray Harris <rharris@shtriallaw.com>

Subject: Data breach - 12170

Good Morning,

The Office of Consumer Affairs and Business Regulation (MA) has received your notification of a data breach dated November 16, 2017 in regards to certain lawsuits alleging asbestos-related injuries. You indicate in your letter that due to the encryption by the ransomware attack, you could not compile a definitive list of persons whose information may have been in the files that are now encrypted. At this time, we would like to know:

-If you have identified the Massachusetts residents that have been affected by this data breach and if so, would you please provide us with the number of affected Massachusetts residents; and

-If residents were identified, a copy of the letter that was sent to the affected Massachusetts residents.

I attach the requirements for Security Breach Notifications under Chapter 93H as a reference for you.

Please feel free to email your response with the missing information, a new letter is not needed. If you have any questions, please let me know.

Thank you,
Anne

Anne Hotchkiss
Executive Assistant to the Undersecretary
Office of Consumer Affairs and Business Regulation
501 Boylston Street
Suite 5100
Boston, MA 02116

Tel 617-973-8701 | Fax 617-973-8799

Schachter Harris, LLP
909 Lake Carolyn Parkway, Suite 1775
Irving, TX 75039

NOTICE OF DATA SECURITY INCIDENT

As a precautionary measure, we are writing to let you know about a data security incident that may involve your personal information received by Schachter Harris, LLP (the "Firm") in the course of defense of litigation alleging asbestos-related injuries in which you or a family member were a plaintiff.

WHAT INFORMATION WAS INVOLVED?

If your information was accessed, the data accessed may have included personal information such as name, address, driver's license number, social security number, military and employment records, medical records, and medical information. The information most likely to be in files containing this information relates to the injured person who was the subject of the suit, but in some cases may relate to family members or those who provided evidence.

WHAT WE ARE DOING:

The Firm is conducting a review of the potentially affected records and computer systems, and the Firm has taken steps to protect data from further unauthorized access, including replacing affected systems and machines. The Firm also is working closely with IT experts and law enforcement to investigate and properly address the incident.

WHAT YOU CAN DO:

Please also review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information.

FOR MORE INFORMATION:

For further information and assistance, please contact the Firm at 214-999-5700 between 9:00 a.m.- 5:00 p.m. (Central) daily.

Steps You Can Take to Further Protect Your Information

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Obtain and Monitor Your Credit Report**

You may also obtain a free copy of your credit report from each of the three major credit reporting agencies by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at <http://www.annualcreditreport.com/requestReport/requestForm.action>. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(800) 685-1111
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 4500
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

- **Consider Filing or Obtaining a Police Report**

You have a right to obtain a police report in regard to this incident. If you are the victim of identity theft, you have the right to contact your local police department to file a report or obtain a copy of one. The report may be filed in the location in which the offense occurred, or the city or county in which you reside. When you file the report, you will be asked to provide as much documentation as possible, including copies of credit reports, and additional information you have.

- **Obtain a Security Freeze**

You have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, cell phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency by sending a written request to each of the three major consumer reporting agencies listed above. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to \$5 to place, lift, or remove the security freeze, unless you are the victim of identify theft and you have submitted a valid police report, investigative report or complaint filed with a law enforcement agency relating to the identify theft incident to the consumer reporting agency.

- **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338).

Additionally, you may obtain information about registering for third-party credit monitoring and alert services advertised as free at the following websites:

- TransUnion (through TrueIdentity) - <https://www.transunion.com/product/trueidentity-free-identity-protection>
- Equifax (through TrustedID Premier) - <https://www.equifaxsecurity2017.com>
- Experian - <https://www.freecreditscore.com>

- **Attorney General Contacts**

Massachusetts Attorney General: (617) 727-2200; <https://www.mass.gov/orgs/office-of-attorney-general-maura-healey>

West Virginia Attorney General: P.O. Box 1789, Charleston, WV 25326. Toll-Free: 1-800-368-8808. Phone: 304-558-8986. Fax: 304-558-0184. consumer@wvago.gov.
<http://www.ago.wv.gov/consumerprotection/Pages/Identity-Theft-Prevention.aspx>